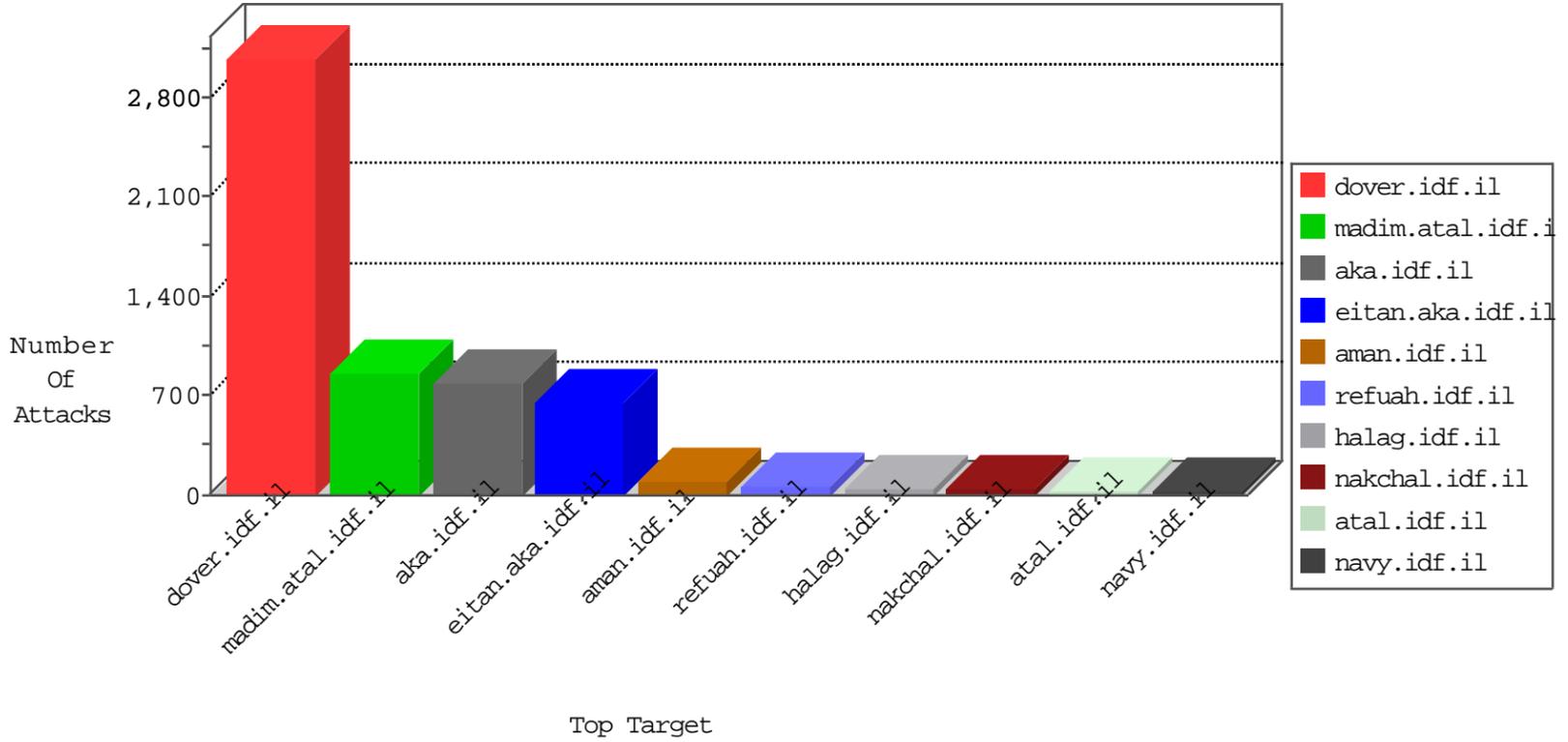


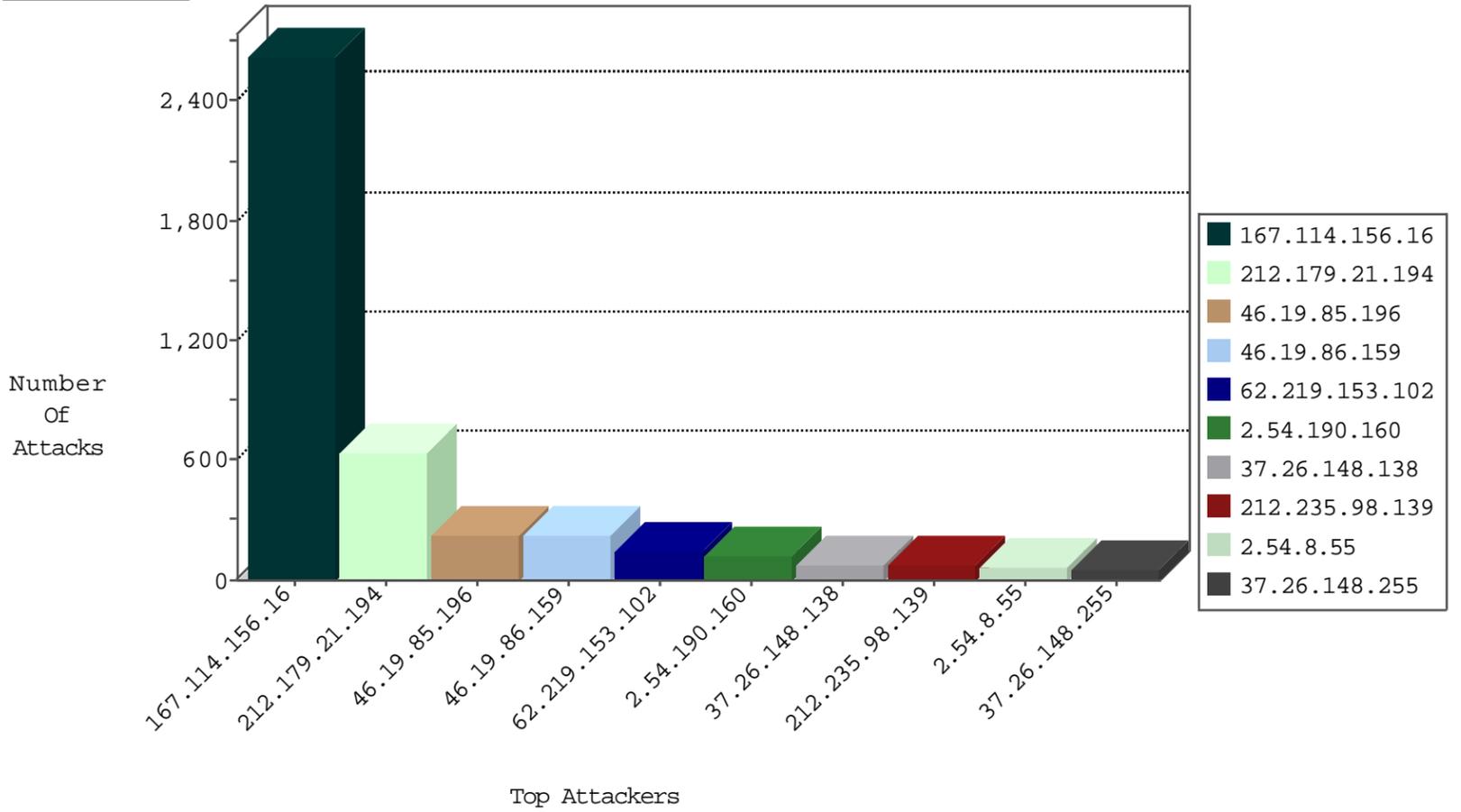
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.66.75	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4507
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3689
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	103
84.109.125.65	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	15
82.145.217.192	Europe	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	5
212.179.64.162	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
118.193.21.98	China	147.237.76.176	test.ncore.idf.i	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
179.177.56.19	Brazil	147.237.72.166	aka.idf.il	C041: HTTP: Access to - index.php?option=com_jce	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.29	147.237.77.216	Israel	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	21
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
94.102.48.195	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.77.19	Ukraine	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.28.226	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.116.82.208	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.6.71.154	147.237.77.179	Poland	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
223.71.218.38	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
132.72.185.88	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.114	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
85.250.90.121	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.57.151	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.158	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.228.137	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
223.71.218.38	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	70
2.54.190.160	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	38
79.183.213.150	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
100.100.3.213		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
2.54.190.160	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	21
37.26.149.206	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.85.29	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
2.54.19.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
100.100.28.123		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	18
46.116.98.44	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
79.180.38.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
31.168.164.162	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
85.250.86.117	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
79.180.38.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
2.54.190.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
2.54.190.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	13
2.54.190.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
62.219.153.102	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.67.164.163	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.198	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.196	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
82.80.154.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.54.190.160	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
185.120.126.74		147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
94.230.86.132	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
100.100.103.221		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
87.69.184.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
82.80.154.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
31.168.118.254	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
80.178.134.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
46.19.86.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.150.161.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.254.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.7.55	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.20.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.237	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.173.170	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
5.102.254.179	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.120.126.74		147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
31.168.156.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.131.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.179.215.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.110.40.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.131.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.203.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.172.135.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	606
46.19.86.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	151
46.19.85.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	112
62.219.153.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	102
46.19.85.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	97
37.26.148.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
46.19.86.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	70
2.54.8.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
37.26.148.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
176.12.137.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
62.219.153.102	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 62.219.153.102	Block	26
95.86.107.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
2.54.28.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
176.13.17.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	6
5.29.180.142	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	4
37.26.148.255	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtStreet in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	3
50.87.207.154	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
2.54.130.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
217.170.205.27	Norway	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
91.109.15.16	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
176.13.6.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
74.114.206.202	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
65.60.26.15	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
89.108.107.58	Russian Federation	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
173.254.77.122	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
50.87.207.154	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
82.80.154.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.52.49.102	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
65.60.26.15	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 65.60.26.15	Block	2
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	2
132.70.66.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sahar	Block	2
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.86.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
74.114.206.202	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
89.108.107.58	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
46.19.85.15	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
173.254.77.122	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
79.180.38.103	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.233	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
217.170.205.27	Norway	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
109.67.164.163	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
91.109.15.16	United Kingdom	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
62.219.137.5	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
74.114.206.202	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
65.60.26.15	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
89.108.107.58	Russian Federation	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2